## **Claims**

## WHAT IS CLAIMED IS:

- 1 1. A method for managing Virtual Private Network (VPN) communications,
- 2 comprising:
- receiving a communication from a local client which is directed to a remote
- 4 client over an insecure network;
- 5 identifying a VPN associated with the communication;
- 6 translating the communication for delivery within the VPN; and
- 7 sending the translated communication via the VPN to a remote transparent
- 8 VPN service, which manages VPN traffic for the remote client.
- 1 2. The method of claim 1 further comprising, processing the method as a local
- 2 transparent VPN service, which manages VPN traffic for the local client.
- 1 3. The method of claim 1 wherein receiving further comprising, directing the
- 2 communication from the local client to the method based on the local client
- attempting to access a defined port, the defined port is associated with a switch or
- 4 router that relays the communication to the method.
- 1 4. The method of claim 1 further comprising, interacting with the remote
- 2 transparent VPN service to manage additional communications between the local
- 3 client and the remote client via the VPN.
- 1 5. The method of claim 4 further comprising, caching data received from the
- 2 remote transparent VPN service in a local cache for accelerated delivery to the local
- 3 client.
- 1 6. The method of claim 1 wherein receiving the communication further
- 2 includes receiving the communication in at least one of a File Transfer Protocol

Attorney Docket No.: 1565.074US1 17

Client Docket No.: IDR-694

- (FTP) format and a Transmission Control Protocol (TCP) format. 3
- 7. The method of claim 1 further comprising, communicating with the remote 1
- transparent VPN service over the insecure network via Secure Sockets Layer (SSL) 2
- or Transport Layer Security (TLS). 3
- A method for managing Virtual Private Network (VPN) communications, 1 8.
- 2 comprising:
- receiving a communication from a local client which is directed to a remote 3
- 4 client associated with a VPN; and
- 5 inspecting the communication for determining whether the communication is
- 6 a request for data that resides in a local cache, and if so, delivering the data to the
- local client, and if not, locating a remote transparent VPN service associated with 7
- the VPN, and wherein the communication is translated into formats used by the 8
- 9 VPN and sent securely over an insecure network to the remote transparent VPN
- service for delivery to the remote client. 10
- 1 The method of claim 8 wherein inspecting further includes establishing 9.
- secure communications with the remote transparent VPN service using at least one 2
- of Sockets Layer(SSL) and Transport Layer Security (TLS). 3
- 1 10. The method of claim 8 wherein inspecting further includes identifying the
- remote transparent VPN service as a service which is managing VPN traffic for the 2
- 3 remote client.
- 1 11. The method of claim 8 wherein receiving further includes intercepting the
- 2 communication issued from the local client by using a router or switch, wherein the
- local client directs the communication to the remote client via the communication 3
- port and the router or switch relays the communication to the processing of the 4

method. 5

> Attorney Docket No.: 1565.074US1 18 **IDR-694**

Client Docket No.:

- 1 12. The method of claim 8 further comprising:
- 2 receiving a response communication from the remote client via the remote
- 3 transparent VPN service, if the communication had been sent via the VPN because
- 4 it could not be satisfied from the local cache;
- 5 translating the response based on the formats of the VPN; and
- 6 delivering the translated response to the local client.
- 1 13. The method of claim 8 further comprising, managing additional
- 2 communications associated with the VPN from one or more different local clients
- 3 which are directed between one or more different remote clients, wherein the remote
- 4 transparent VPN service manages the additional communications on behalf of the
- 5 one or more different remote clients.
- 1 14. The method of claim 8 wherein receiving further includes intercepting the
- 2 communication after detecting that the local client is transmitting the
- 3 communication with a non-Hypertext Transfer Protocol (HTTP).
- 1 15. The method of claim 8 further comprising, interacting with the remote
- 2 transparent VPN service with mutually signed certificates that are exchanged
- 3 between the method and the remote transparent VPN service during the interactions.
- 1 16. A Virtual Private Network (VPN) managing system, comprising:
- a remote transparent VPN service; and
- a local transparent VPN service, wherein local transparent VPN service
- 4 intercepts and manages VPN traffic on behalf of one or more local clients and
- 5 services communications of those local clients with data in a local cache, if
- 6 available, and if the data is not available in the local cache, the local transparent
- 7 VPN service transmits the communications securely to the remote transparent VPN
- 8 service for delivery and servicing by one or more remote clients which the remote
- 9 transparent VPN service manages.

Attorney Docket No.: 1565.074US1 19

Client Docket No.: IDR-694

- 1 17. The VPN managing system of claim 16 wherein the local transparent VPN
- 2 service and the remote transparent VPN service interact via at least one of Secure
- 3 Sockets Layer (SSL) and Transport Layer Security (TLS).
- 1 18. The VPN managing system of claim 16 wherein the local transparent VPN
- 2 service intercepts local VPN traffic on behalf of the one or more local clients by
- 3 inspecting Transmission Control Protocol (TCP) or File Transfer Protocol (FTP)
- 4 communications originating from the one or more local clients.
- 1 19. The VPN managing system of claim 16 wherein the local transparent VPN
- 2 service intercepts the VPN traffic through a router or switch which is configured to
- 3 relay communications on a defined port to the local transparent VPN service.
- 1 20. The VPN managing system of claim 16 wherein communications between
- 2 the local and remote transparent VPN services occur with mutually exchanged
- 3 certificates.
- 1 21. A Virtual Private Network (VPN) managing system, comprising:
- 2 a communication port; and
- a local transparent VPN service, wherein VPN communications directed to
- 4 the communication port are relayed to the local transparent VPN service, the local
- 5 transparent VPN service attempts to service the VPN communications from local
- 6 cache and if attempts fail, the local transparent VPN service securely communicates
- 7 with a remote transparent VPN service via an insecure network to service the VPN
- 8 communications.
- 1 22. The VPN managing system of claim 21 further comprising a router or switch
- which relays the VPN communications to the local transparent VPN service.
- 1 23. The VPN managing system of claim 21, wherein the system resides on a
- 2 server and services a plurality of local clients associated with the VPN

Attorney Docket No.: 1565.074US1 20

Client Docket No.: IDR-694

- 3 communications.
- 1 24. The VPN managing system of claim 21 wherein the system resides on a
- 2 single client.
- 1 25. The VPN managing system of claim 21 wherein the local transparent VPN
- 2 service translates and services the VPN communications on behalf of a one or more
- 3 of local clients.
- 1 26. The VPN managing system of claim 25 wherein the remote transparent VPN
- 2 service translates and service the VPN communication on behalf of a one or more of
- 3 remote clients.

Attorney Docket No.: 1565.074US1 21